# AMENDMENTS TO THE CLAIMS

The listing of claims will replace all prior versions, and listings, of claims in the application:

1-25.   (Cancelled)

26.    (Currently Amended) A computer-readable medium having stored thereon a data structure having a plurality of fields, the data structure comprising:

a plurality of client identifier fields that each identify a client computer system that is connected to a server computer system; and

for each identified client computer system, the data structure further comprising at least one authentication field that identifies an authentication method to be used by the server computer system for authenticating the client computer system upon receiving a request from the client computer system for service, the authentication method having been selected by a controlling client computer system that is different from the client computer system based on authentication abilities and access rights of the client computer system so that the client computer system need not unnecessarily reveal secret information.

27.    (Previously Presented) The computer-readable medium in accordance with Claim 26, wherein each client identifier field identifies a different single client computer system.

28.    (Previously Presented) A computer-readable medium as recited in claim 26, wherein the server computer system has access to the data structure prior to receiving the request from the client computer system.

29.    (Previously Presented) A computer-readable medium as recited in claim 26, wherein the data structure is further configured to be altered upon being stored, so as to allow a client computer system to use additional authentication methods.

30.    (Currently Amended) A method in a server computer of authenticating client computer systems, the method comprising:

   receiving from a controlling client computer system an instruction that indicates an authentication methodology that is to be used to authenticate a client computer system that is different from the controlling client computer system, the authentication methodology being selected from multiple authentication methodologies based on authentication abilities and access rights of the client computer system; and

   upon receiving a request from the client computer system to access a service of the server computer, authenticating the client computer system using the indicated authentication methodology.

31.    (Previously Presented) The method of claim 30 wherein the instruction indicates that multiple authentication methodologies can be used to authenticate the client computer system and wherein the client computer system is authenticated using one of the indicated authentication methodologies.

32.    (Previously Presented) The method of claim 30 wherein the instruction indicates that the authentication methodology is to be used to authenticate multiple client computer systems and wherein the multiple client computer systems are authenticated using the indicated authentication methodology.

33.    (Previously Presented) The method of claim 30 wherein the instruction indicates multiple authentication methodologies can be used to authenticate multiple client

computer systems and wherein the multiple client computer systems are authenticated using one of the indicated authentication methodologies.

34.    (Previously Presented) The method of claim 30 wherein the authentication methodology is an assertion authentication.

35.    (Previously Presented) The method of claim 30 wherein the authentication methodology is a basic HTTP authentication.

36.    (Previously Presented) The method of claim 30 wherein the authentication methodology is digest authentication.

37.    (Previously Presented) The method of claim 30 wherein the authentication methodology is an NTLM authentication.

38.    (Currently Amended) A method in a controlling client computer system for providing authentication methodologies to a server computer system, the method comprising:

    generating an instruction that indicates an authentication methodology that is to be used to authenticate a client computer system that is different from the controlling client computer system, the authentication methodology being selected from multiple authentication methodologies based on authentication abilities and access rights of the client computer system; and

    sending the generated instruction to the server computer system so that upon receiving a request from the client computer system to access a service of the server computer system, the server computer system can authenticate the client computer system using the indicated authentication methodology.

39.    (Previously Presented) The method of claim 38 wherein the instruction indicates that multiple authentication methodologies can be used to authenticate the client computer system and wherein the client computer system is authenticated by the server computer system using one of the indicated authentication methodologies.

40.    (Previously Presented) The method of claim 38 wherein the instruction indicates that the authentication methodology is to be used to authenticate multiple client computer systems and wherein the multiple client computer systems are authenticated by the server computer system using the indicated authentication methodology.

41.    (Previously Presented) The method of claim 38 wherein the instruction indicates multiple authentication methodologies can be used to authenticate multiple client computer systems and wherein the multiple client computer systems are authenticated by the server computer system using one of the indicated authentication methodologies.

42.    (Previously Presented) The method of claim 38 wherein the authentication methodology is an assertion authentication.

43.    (Previously Presented) The method of claim 38 wherein the authentication methodology is a basic HTTP authentication.

44.    (Previously Presented) The method of claim 38 wherein the authentication methodology is digest authentication.

45.    (Previously Presented) The method of claim 38 wherein the authentication methodology is an NTLM authentication.

46.    (Currently Amended) A computer-readable medium containing instructions for controlling a server computer system to authenticate entities, by a method comprising:

receiving from a controlling entity an instruction that indicates an authentication methodology that is to be used to authenticate an entity, the authentication methodology being selected from multiple authentication methodologies based on authentication abilities of the entity that indicate which authentication methodologies are supported by the entity, the controlling entity being different from the entity; and

upon receiving a request from the entity to access a service of the server computer system, authenticating the entity using the indicated authentication methodology.

47.    (Previously Presented) The computer-readable medium of claim 46 wherein the instruction indicates that multiple authentication methodologies can be used to authenticate the entity and wherein the entity is authenticated using one of the indicated authentication methodologies.

48.    (Previously Presented) The computer-readable medium of claim 46 wherein the instruction indicates that the authentication methodology is to be used to authenticate multiple entities and wherein the multiple entities are authenticated using the indicated authentication methodology.

49.    (Previously Presented) The computer-readable medium of claim 46 wherein the instruction indicates multiple authentication methodologies can be used to authenticate multiple entities and wherein the multiple entities are authenticated using one of the indicated authentication methodologies.

50.    (Previously Presented) The computer-readable medium of claim 49 wherein the authentication methodology is selected from a group consisting of an assertion

authentication, a basic HTTP authentication, a digest authentication, and an NTLM authentication.